Masthead Logo

Indiana Journal of Global Legal Studies

Volume 26 | Issue 1 Article 11

2-15-2019

Younger Generations are Infected by Continuous Socialization to Accept Diminished Privacy: A Global Analysis of How the United States' Constitutional Doctrine Is a Main Contributor to Eroded Privacy

Tiffany Kim

Indiana University Maurer School of Law, kimti@iu.edu

Younger Generations are Infected by Continuous Socialization to Accept Diminished Privacy: A Global Analysis of How the United States' Constitutional Doctrine Is a Main Contributor to Eroded Privacy

TIFFANY KIM*

INTRODUCTION

Since the nineteenth century, privacy concerns have increased with the growth of technology. The invention of instantaneous photography, coupled with the enlarged presence of press, was met with concerns of degraded privacy.[1] Society has formed expectations of privacy, but as time passes, those expectations continue to diminish. Younger generations have been socialized to accept lessened levels of privacy in this digitalized world of mass data and connectivity.[2]

Individual privacy expectations vary globally. The construction of China's government and culture produces a lesser expectation of individual privacy than that of the United States. As outlined in the U.S. Constitution, U.S. citizens expect freedom from government surveillance without an authorized warrant,[3] which is inconsistent with the privacy expectations of Chinese citizens.

This essay first discusses an article by Cyrus Farivar,[4] followed by an article by Ava Kofman, [5] both of which relate to mass data collection

* Symposium Editor, Indiana Journal of Global Legal Studies, Volume 26; J.D. Candidate, 2019, Indiana University Maurer School of Law—Bloomington; B.S., Criminal Justice, 2016, Grand Valley State University.

1. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (discussing the evolution of privacy law).

2. I use the word "connectivity" to describe the abundance of devices that we use on a daily basis that connect to the Internet, including our vehicles, TVs, phones, watches, toasters, and bed comforters.

3. *See* U.S. CONST. amend. IV.

4. Cyrus Farivar, *Axon Wants You (Yes, You!) to Submit Photos, Videos to Police*, ARS TECHNICA (Oct. 19, 2017, 5:29 PM), https://arstechnica.com/tech-policy/2017/10/axon-wants-you-yes-you-to-submit-photos-videos-to-police/.

Indiana Journal of Global Legal Studies Vol. 26 #1 (Winter 2019)

in the United States. This note will discuss how the expectation of privacy continues to diminish as younger generations are being socialized to willingly accept a lesser degree of individual privacy. Additionally, this note will examine an article by Rachel Botsman,[6] which describes a Chinese mass data collection initiative currently underway that—were it to be implemented in the United States—would perceivably be categorized as a farfetched, outrageous initiative. Finally, this essay analyzes the grave effects new technologies and practices will have on diminishing privacy and asserts that China's perceivably outrageous mass data collection practices would survive U.S. constitutional bars if the current constitutional doctrine is applied.

AXON CITIZEN WILL FURTHER SOCIALIZE PEOPLE TO ACCEPT DIMINISHED PRIVACY

In an age where the vast majority of individuals possess a camera in their pocket on a daily basis, concerns for privacy are drastically heightened. Axon, a technology company that is the largest provider of body-worn cameras and data storage products to American law enforcement agencies, announced its launch of Axon Citizen.[7] Essentially, Axon Citizen is a "public safety portal[,]"[8] which allows anyone to share information with law enforcement by submitting text, video, and audio files to Evidence.com, a law enforcement cloud storage interface.[9] Axon's product gained support and investment because it gives police more technology and resources for information gathering and would cut investigation expenses.[10]

Although Axon Citizen and Evidence.com have shown potential benefits for solving crime, there are prominent privacy concerns that accompany the unregulated mass data collection initiative. The standard policing practices and procedures for implementing and operating the public safety portal are still ambiguous with numerous questions left unanswered. For instance, what is the policy regulating the length of data retention? "Will either Axon or the individual agency

5. Ava Kofman, *Taser Wants to Build an Army of Smartphone Informants*, THE INTERCEPT (Sept. 21, 2017, 11:54 AM), https://theintercept.com/2017/09/21/taser-wants-to-build-an-army-of-smartphone-informants/.

6. Rachel Botsman, *Big Data Meets Big Brother as China Moves to Rate Its Citizens*, WIRED (Oct. 21, 2017), http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion.

7. *See* Farivar, *supra* note 4 (describing how Axon announced the launch of Axon Citizen, a public safety portal for evidence upload, on Thursday, October 19, 2017).

8. *Id.*

9. *Id.*

10. *See id.*

be pulling out data that's unrelated to the particular event being reported, whether it's license plate data in the background or individuals tagged down the line by facial recognition software? Will they be mined for leads for other crimes?"[11]

If citizens can submit any video they captured, does the distinction between a public and a private setting matter? In 1958, Hannah Arendt asserted that absolute privacy is only obtainable within the four walls of the home.[12] The decision in *Gill v. Hearst Publishing Co.* reflects this concept of privacy, where a husband and wife were captured by a photographer as they were seated in an affectionate pose at a farmers market.[13] The couple did not know or consent to their photograph being taken, let alone consent to it being published and widely circulated, yet the court held that there was no privacy violation because they were in public.[14] To the contrary, in *Daily Times Democrat v. Graham*, a mother who escorted her two young children through a fun house at the fair was photographed as she exited the fun house with her dress blown up by the air, and the court held the defendant who published the photograph violated the mother's right to privacy.[15] The court concluded that being in the public sphere did not provide an absolute defense because such a mechanical application of legal principles would produce an illogical conclusion.[16] Here, the court focused on the obscene nature of the photograph. Synthesizing the *Gill* and *Graham* decisions, if you are in public, you do not have a right to privacy in regards to having your photograph taken, unless the photograph is obscene.

The Supreme Court attempted to clarify privacy in public as it relates to Fourth Amendment protections by describing how society has formed a reasonable expectation of privacy in certain public places. In *Katz v. United States*, the government placed a recording device outside a telephone booth—without a warrant.[17] Justice Harlan's concurring opinion declared that the defendant did have a reasonable expectation

---

11. Farivar, *supra* note 4.

12. *See generally* HANNAH ARENDT, THE HUMAN CONDITION (1958) (discussing the relationship between the public and private realms and how individual privacy is achieved).

13. *See* Gill v. Hearst Publ'g Co., 253 P.2d 441, 441-42 (Cal. 1953).

14. *See id.* (noting that the picture taken was not offensive or shocking to the ordinary sense of decency).

15. *See* Daily Times Democrat v. Graham, 162 So. 2d 474, 474-75 (Ala. 1964) (noting that there was no legitimate news value in the photograph and the photograph was embarrassing and obscene).

16. *See id.* at 478.

17. *See* Katz v. United States, 389 U.S. 347, 348-50 (1967).

of privacy inside a public phone booth where he had the door closed.[18] Harlan's concurrence promulgated the reasonable expectation of privacy test, which calls for a two-step analysis: a subjective expectation of privacy and whether society is willing to accept that subjective expectation as objectively reasonable.[19] In this decision, the Supreme Court shifted the expectation of privacy to anywhere a person might reasonably expect privacy, not simply a private-versus-public-sphere categorization.

However, the reasonable expectation of privacy test requires the court to assess the societal views of privacy, which has contributed to the diminished privacy protections society is now forced to accept.[20]

> Societal expectations guide judicial rulings, which guide societal expectations, and so on. That circularity is especially problematic here at the onset of the Information Age because digital communications and data are only beginning to take their place in society. Expectations about privacy in this medium are still taking form, and the technology continues to change, so there is simply no objectively reasonable sense of privacy for judges to discover.[21]

The growth of technology, especially readily available cameras, contributes to the simple expectation that a person cannot achieve privacy in public spaces, which is a further deviation from *Katz*. Furthermore, the categorization of public-versus-private does not provide the flexibility that is needed, especially regarding information privacy and data collection. Given the current digital society, privacy should not hinge on the distinction between the public or private sphere.[22]

---

18. *See id.* at 360-61 (Harlan, J., concurring) (reasoning that even though an individual was in public place, a person making a phone call with the telephone booth door shut could rely upon the protections of the Fourth Amendment).

19. *See id.*

20. *See* Brief for the Competitive Enterprise Inst. et al. as Amici Curiae Supporting Petitioner at *14, Carpenter v. United States, 137 St. Ct. 2211 (2017) (No. 16-402), 2017 WL 2407484 (petition of writ of certiorari granted) (discussing how the reasonable expectation of privacy test is insufficient and detrimental to individual privacy protections).

21. *Id.*

22. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1132 (2002) (asserting that public and private categorization is not effective because it changes depending on the time and subcultures).

Axon's Evidence.com will contribute to the socialization of accepting less privacy. People will accept the fact that if they are in public, they could be recorded, and the content about them could be stored in a database. Courts have guided this socialization of diminished privacy by defining the distinction between public-versus-private, especially in the context of government actors versus private actors.

In addition to the public and private distinction, the judiciary created the Third-party Doctrine, which essentially diminished the privacy expectation individuals have in the information that is relayed to a third-party. The Court promulgated the Third-party Doctrine in *United States v. Miller*. The government issued blank form subpoenas to bank presidents where the defendant had accounts. The banks provided documents related to the defendant's accounts to the government that were used to convict the defendant of four counts of possession of an unregistered still and failure to pay taxes.[23] The Fifth Circuit reversed the conviction.[24] The court held that the depositor's Fourth Amendment rights were violated in this instance because banks must comply with the Bank Secrecy Act when maintaining records, and the records were obtained by a defective subpoena.[25] The Supreme Court, however, disagreed with the Fifth Circuit opinion reasoning that despite the Bank Secrecy Act, the depositor has no reasonable expectation of privacy in information that he provides to a third party.[26] The court further stated its holding.

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[27]

Contrary to the *Miller* Court's declaration that a depositor cannot have a reasonable expectation of privacy in information that is conveyed to a third party, the lack of privacy alarmed a clear bulk of society, which suggests an objective reasonable expectation of privacy would not

---

23. *See* United States v. Miller, 425 U.S. 435, 436-37 (1976).

24. *Id.* at 437 (describing the procedural history and how the Court of Appeals held that the bank records must be suppressed).

25. *Id.*

26. *See* Miller, 425 U.S. at 443 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

27. *Id.*

be so farfetched.[28] Take Justice Marshall's dissent in *Smith v. Maryland* for example.[29] In an investigation of the defendant, who was suspected of robbery and making threatening phone calls, the police requested that the telephone company install a pen register—without a warrant.[30] The majority held that there was no Fourth Amendment violation because there was no reasonable expectation of privacy in the phone numbers dialed, which were transmitted to the telephone company.[31] The majority further declared that even if the defendant truly did have a subjective expectation of privacy in the numbers he dialed, the expectation is not one that society is willing to except.[32] Justice Marshall, however, was astonished by the majority's opinion that individuals could not reasonably expect privacy in the phone numbers that are dialed merely because the phone numbers are voluntarily turned over to a third party.[33] The majority reasoned that individuals assume the risk of voluntarily disclosing information to a third party, but Justice Marshall asserted that such an analysis is wrong because it assumes people have a choice.[34]

Consistent with Justice Marshall's lack-of-choice reasoning, Axon Citizen creates an *autonomy trap* that will be detrimental to society's privacy expectations. An *autonomy trap* exists when an individual cannot exercise autonomy because there are simply no other reasonable options.[35] For example, disclosing cell phone data to the cell phone provider is unavoidable, and one cannot choose to use a different cell phone provider to avoid disclosing the phone numbers that are dialed; therefore, this could be categorized as an autonomy trap. If an

---

28. *See generally* Burrows v. Superior Court, 529 P.2d 590 (1974) (holding, as a matter of state constitutional law, that bank depositors have a sufficient expectation of privacy in their bank records).

29. *See* Smith v. Maryland, 442 U.S. 735, 748-51 (1979) (Marshall, T., dissenting) ("It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.").

30. *Id.* at 737 (describing a pen register as a device that records the numbers pressed when dialing the telephone).

31. *Id.* at 742.

32. *Id.* at 744 ("When [petitioner] used his phone, [he] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

33. *See id.* at 748-50 (Marshall, J., dissenting).

34. *See id.* at 750 ("[U]nless a person is prepared to forgo use of what to many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."); *see also* United States v. Carpenter, 819 F.3d 880, 894-95 (6th Cir. 2016) (Stranch, J., concurring) (noting that the third-party doctrine is not suitable for modern technology).

35. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 821 (2000).

individual does not want to consent to potentially being video recorded and uploaded to a privatized, obscure database, the only choice is to never go out in public. Although many supporters of Evidence.com advocate that it will only be used to investigate crime, grave privacy concerns are absolutely justified when Evidence.com is an unregulated, privatized database.[36]

First, if body-camera footage is uploaded to Evidence.com, it could include innocent individuals who are now part of a perpetual line-up, indefinitely.[37] Second, it is unclear how Axon intends to exploit the data.[38] In the aggregate, data is powerful. Justice Brennan and Justice Marshall even recognized the close relationship between aggregation and power in the information discarded in a residential trashcan. In *California v. Greenwood*, police searched, without a warrant, opaque garbage bags left for collection in front of the defendant's home.[39] The court held that items abandoned or exposed to the public, like garbage in a trashcan, have been conveyed to a third party and that there is no reasonable expectation of privacy in a personal garbage can sitting on the curb of a home.[40] Yet two dissenting justices recognized that "a single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it."[41] Information in the aggregate, whether obtained from a trashcan or from third parties, reveals intimate details about an individual's life and creates a platform of commercial power over citizens' privacy.

PRIVATIZATION OF A PUBLIC SERVICE WILL FURTHER SOCIALIZE PEOPLE TO ACCEPT DIMINISHED PRIVACY

Axon's new Public Evidence Product, or Evidence.com, benefits the law enforcement tech giant with yet another source of data the company can monetize. The CEO of Axon refers to the platform as a "dropbox for cops" because it will allow citizens to submit photos or video evidence to

---

36. *See* Farivar, *supra* note 4.

37. *See generally* CLARE GARVIE ET AL., GEO. L. CTR. ON PRIVACY & TECH., THE PERPETUAL LINE-UP (2016) (discussing the grave effects of unregulated mass data collection to be used for facial recognition, producing vast constitutional and civil liberties violations).

38. *See* Farivar, *supra* note 4.

39. *See* California v. Greenwood, 486 U.S. 35, 37-39 (1988) (Brennan, J., dissenting).

40. *See id.* at 41 (majority opinion) ("[S]ociety would not accept as reasonable respondents' claim to an expectation of privacy in trash left for collection in an area accessible to the public . . . .").

41. *See id.* at 50 (Brennan, J., dissenting) (describing the intimate details a search of a trash can reveal, including activities associated with the "sanctity of a man's home and the privacies of life" which is at the epicenter of Fourth Amendment protections).

Evidence.com, which will ultimately help law enforcement in crime solving and gathering a "fuller point of view from the public."[42] The potential benefits of enhanced investigation techniques are met with grave concern for the traditional public service role becoming privatized.[43] While the Intercept article discusses the same Axon Citizen product in the Ars Technica article analyzed above, the Intercept article expanded on privacy implications, potential intentions of Axon, and video tactics that the American Civil Liberties Union (ACLU) and Witness have employed to combat police brutality.

Initially, body cameras were implemented to ensure police accountability; however, the cameras are actually being operationalized as surveillance tools for police.[44] Stanley Benn asserts that surveillance, or secret watching, in itself does not cause harm; therefore, surveillance should not be based on harm done but rather on the principle of respect for others.[45] Conversely, Julie Cohen proclaims privacy is of the highest value because it is crucial to constitutional protections, such as First Amendment freedoms, and promotes the development of a civil society where individuals are autonomous and free to explore eccentric individuality.[46] Cohen's perspective analyzes the purpose of privacy as a collective right to protect democracy. Surveillance is extremely harmful to a democratic society because it can chill an individual's freedom of expression and exercise of civil liberties.[47]

Younger generations tend to distance themselves from the realities of surveillance via mass data collection because it is not physical

---

42. *See* Kofman, *supra* note 5.

43. *See id.* ("This [trend] is happening in a million different ways, whether it's people photographing evidence of crimes on Facebook or apps that allow you to take photographs and report other people's parking violations. This is becoming more prominent, and more and more minute offenses are being drawn into this vast surveillance dragnet.").

44. *See id.* (discussing how body cameras were initially advocated for the purpose of increasing transparency and building trust between police and the public, but "body camera footage has rarely been used to indict officers for brutality" and instead used to turn beat cops into "walking surveillance cameras.").

45. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 53 (5th ed. 2015) (quoting Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, from *Nomos XIII: Privacy* (J. Ronald Pennock & J.W. Chapman eds., 1971)).

46. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424-25 (2000) ("The recognition that anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association—decision that other might be chilled by unpopularity or simple difference—is part of our constitutional tradition.").

47. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) (discussing the importance of freedom for intellectual expression, such as forming opinions on politics or social issues, and how surveillance of those activities is detrimental when it deters an individual from exercising their freedom of expression in communicating with others while forming opinions).

surveillance; therefore, it is perceived as less intrusive or not intrusive at all. Axon claims, however, that by conducting analytics on its video database, such as Google or Amazon analytics, it will soon have the capability to "anticipate criminal activity."[48] It may be difficult to fathom how this capability will actually be operationalized, but given the relationship Axon has with the government, this type of analytics will likely have drastic effects on privacy, not to mention the varied and numerous racial profiling algorithms that are already a significant issue with facial recognition software.[49]

Axon makes money through government subscriptions to their database;[50] given this dynamic, it is reasonable to assume the anticipated criminal activity analytics will be at the disposal of law enforcement but lack Fourth Amendment protections. Unlike technology companies like Google, who do not voluntarily turn over information on citizens without a valid search warrant or motion to compel,[51] Axon's clients are public sector entities. Axon is creating capabilities for law enforcement, not the public; such a relationship not only lacks incentive for Axon to protect the privacy of citizens but deters the protection of privacy. This dynamic bestows power on the commercial and government entities over the individual autonomy, which can lead to coercion.[52]

Axon will be analogous to facial recognition software that searches databases containing photos from mugshots, driver's licenses, and passports.[53] Axon Citizen and Cop Dropbox, or Evidence.com, are going to further expand the perpetual line-up that lacks accountability, accuracy, standard protocols, and, most worrisome of all, Fourth

48. Kofman, *supra* note 5.

49. *See generally* GARVIE ET AL., *supra* note 35 (discussing the grave effects of unregulated mass data collection to be used for facial recognition, producing vast constitutional and civil liberties violations, specifically with targeting racial minorities).

50. *See* Kofman, *supra* note 5.

51. The State of Vermont Superior Court, Addison Unit reviewed three similar issues regarding search warrants and granted the government's motion to compel Google to produce all data described in the search warrant because Google did not voluntary turnover the information requested. Google's involuntariness is reflected in three different 2017 *In re* Search Warrant cases: No. 16-MB-004413 (Addison Unit); No. 17AG000003 (Chittenden Unit); and No. 15AG000082 (Washington Unit).

52. *See* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 114-15 (2007) ("First Amendment activities are implicated by a wide array of law enforcement data-gathering activities.").

53. *See* CLARE GARVIE ET AL., *supra* note 37, at 12-15 (describing the FBI's Next Generation Identification Interstate Photo System, the largest face recognition database in the country, and how it contains approximately 411.9 million photos of mugshots, drivers' license, and expanding to the State Department's passport database).

Amendment protections.[54] The majority of facial recognition programs do not require a police officer to obtain a warrant before a search is conducted.[55]

Where every smart device with a camera can record within a split second and act as a minute-by-minute informant for the government, it becomes worrisome that Fourth Amendment protections are subpar. The reality is that Axon's facial recognition and analytics that anticipate criminal activity are real-time government surveillance. Take major metropolitan cities—like Chicago—for example. The city is a place where the government would have a "fuller point of view from the public," as Axon promotes,[56] if facial recognition software was installed on Chicago's camera networks since it is equipped with 10,000 surveillance cameras.[57] The activation of facial recognition software would empower the government to "track someone's movements retroactively or in realtime, in secret, and by using technology that is *not* covered by the warrant requirements of existing state geolocation privacy laws."[58]

Surveillance technology that does not require a physical intrusion, such as installing a GPS location tracker to a person, is perceived as less harmful, but the outcomes are just as severe. In *United State v. Jones*, law enforcement agents were investigating the defendant for trafficking in narcotics.[59] While the defendant's car was parked in a public lot, the government installed a GPS tracking device on the undercarriage and tracked his location for twenty-eight days—without authorization of a valid warrant.[60] The Supreme Court held that putting a GPS tracker on the defendant's vehicle for twenty-eight days, which exceeded the ten day warrant, violated the defendant's Fourth Amendment protections.[61] In her concurrence, Justice Sotomayor

---

54. *See generally* CLARE GARVIE ET AL., *supra* note 37 (discussing the specific deficiencies of unregulated, mass data collection to be used for facial recognition, and how they are producing vast constitutional and civil liberties violations).

55. *See* CLARE GARVIE ET AL., *supra* note 37, at 35 ("To date, however, not a single state or federal court has considered the question of whether a face recognition search constitutes a search for the purpose of the Fourth Amendment, or an analogous provision in a state constitution.").

56. Kofman, *supra* note 5.

57. *See* CLARE GARVIE ET AL., *supra* note 37, at 22 ("In a city equipped with real-time face recognition, every person who walks by a street surveillance camera—or a police worn body camera—may have her face searched against a watchlist.").

58. *Id.*

59. *See* United States v. Jones, 565 U.S. 400, 402-04 (2012).

60. *See id.* at 403-04.

61. *See id.* at 404 (emphasizing that there was a physical intrusion when the government placed the GPS device on the defendant's car); *see id.* (Sotomayor, J., concurring) (noting that physical intrusion in not a requirement to many forms of

recognized that knowing the government is watching chills associational and expressive freedoms, which should be taken into account for societal expectations.[62] Justice Sotomayor perceives one purpose of privacy is the collective right of protecting democracy, similar to Julie Cohen's perspective.[63]

Facial recognition in camera networks and anticipatory analytics of criminal activity will leave no room for obscurity or anonymity. Although these cameras are in public places and generally courts do not recognize a reasonable expectation of privacy in public,[64] an individual should still have the autonomy to seek obscurity and anonymity in public places by merging into the situational landscape.[65] The distinction between private and public figures goes to show that society expects the freedom to seek obscurity or anonymity, even in public places.[66] Society reasonably expects more privacy as a private citizen in public than a public figure or celebrity. Yet, in a society saturated with cameras and technology like Axon's, the societal expectation of privacy will continue to deteriorate.

Furthermore, the ACLU and Witness, a video advocacy organization, are using the same type of software applications that Axon is promoting to record police interactions for accountability purposes.[67] The ACLU's mobile application automatically uploads a cell phone video to a server in real time.[68] In addition to Axon and the government

---

surveillance these days and putting more emphasis on the precision of a GPS device and the length it was employed without an authorized warrant).

62. *See* Jones, 565 U.S. at 416 (Sotomayor, J., concurring).

63. *See* Cohen, *supra* note 46, at 1425. (describing how freedom of intellectual expression is essential to a free, democratic nation).

64. *See, e.g.,* Gill v. Hearst Publ'g Co., 253 P.2d 441 (Cal. 1953) (noting that a picture taken in a public place has no reasonable expectation of privacy); *see also, e.g.,* Neff v. Time, Inc., 406 F. Supp. 858 (W.D. Pa. 1976) (noting Neff was photographed in a sporting event, a public place where there is not a reasonable expectation of privacy).

65. *See generally* ALAN F. WESTIN, PRIVACY AND FREEDOM (1967) (describing privacy in various states, such as solitude, intimacy, anonymity, reserve, and functions of privacy as personal autonomy, individuality, emotional release of social roles, and limited and protected communications).

66. *See* SOLOVE & SCHWARTZ, *supra* note 45, at 7; *see also generally* New York Times v. Sullivan, 376 U.S. 254 (1964) (discussing how public figures should expect less privacy than private individuals).

67. *See* Kofman, *supra* note 5 (responding to failures to release police body camera footage and police purposely switching off or failing to activate body cameras, advocacy organizations deployed their own apps and resources to capture police interactions and implement mass video collection).

68. *Id.*

mobilizing facial recognition software, the ACLU maintains its own cache of video surveillance too.[69]

As more entities begin to utilize real-time video surveillance technology and it becomes more accessible to the general public, the Fourth Amendment will fail to protect citizens. In *Kyllo v. United States*, the police used a thermal imager to scan the defendant's house for high-intensity lamps that would indicate marijuana production—without a warrant.[70] The court held that the use of a sense-enhancing technology to obtain information regarding the interior of the home was a violation of the Fourth Amendment and grounded its decision on the fact that the device was not in general use and that the sense-enhancing technology was targeted in an area of utmost importance for privacy protections, the sanctity of the home.[71] To the contrary, in *Dow Chemical v. United States*, the company denied the Environmental Protection Agency (EPA) a second inspection, so the EPA hired an aerial photographer to fly an aircraft over the facility; yet, the court held that such surveillance was not in violation of the Fourth Amendment.[72] The court reasoned that the photographs did not reveal intimate details sufficient to raise constitutional concerns and further described that a disparity exists between a home and a commercial property.[73]

Applying the reasoning in *Kyllo* and *Dow* to a Fourth Amendment analysis for Axon's technology produces grave outcomes. If more entities use real-time video surveillance, facial recognition, and anticipatory criminal activity analytics, it could be declared a device in general use (unlike the thermal imager in *Kyllo*) and be deprived of Fourth Amendment protections. The absence of intimate details in the *Dow* reasoning could lead to holdings that video surveillance does not reveal anything private, because there is no expectation of privacy in public. The growth of surveillance technologies, coupled with the lack of

---

69. *Id.* (describing the purpose of the ACLU photo and video cloud cache is to enhance police accountability and combat the insufficiency of inadequate police body cameras, since the body worn cameras are not being used effectively for police transparency).

70. Kyllo v. United States, 533 U.S. 27, 29-31 (2001) (discussing the capabilities of a thermal imager to penetrate through the walls of a home and gain intelligence, such as the heat levels used to detect presence of human bodies or in this case, growing lamps).

71. *Id.* at 33-34 ("It would be foolish to contend that the degree of privacy secured to citizens by the *Fourth Amendment* has been entirely unaffected by the advance of technology.").

72. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986) (describing that the aerial photographer was acquired to capture photographs of the commercial complex that the EPA was denied access to for a second inspection).

73. *See Id.* at 231 (noting that the photographs were similar to those commonly used in mapmaking and any person with an airplane would be able to take the same type of aerial pictures).

oversight and Fourth Amendment protections, will continue to erode privacy expectations.

CHINA'S SURVEILLANCE CAPITALISM TURNED TO SOCIAL CONTROL IS NOT A FARFETCHED REALITY FOR THE UNITED STATES

China is launching a social credit system that aims to tie each individual with a numerical score that reflects their social trustworthiness.[74] This may seem farfetched to Westerners, however, the United States has implemented Credit Scores—numerical calculations describing a person's ability to secure loans, financial well-being, and much more, for more than seventy years.[75] Mass data collection provides the means to accomplish China's social score system: where such a score will effect what people may do, where they may go, who they may associate with, and virtually all aspects of life.[76] In a world of mass data collection, every transaction initiated online or with a credit card will be monitored and evaluated; from time spent at locations, to interactions with others, as well as reading, will be monitored and evaluated as well.[77] This concept of mass data collection is not so farfetched considering the capabilities of data giants like Google, Facebook, health tracking apps like Fitbit, and all of the *Internet of Things* devices that are only beginning to saturate daily life. "But now imagine a system where all these behaviours are rated as either positive or negative and distilled into a single number, according to rules set by the government. That would create your Citizen Score and it would tell everyone whether or not you were trustworthy."[78]

China's social score system will negatively affect the entire population by altering all facets of human behavior. Chinese citizens have no opt out option; they are forced to engage with the scoring system;[79] and it would behoove them to take it seriously. Their score will determine eligibility for a job, loan, where their children will be able to go to school, or even who will be willing to associate with them, as a friend, a dating partner, or even just an acquaintance.[80] Monitoring and evaluating shopping habits of an individual can result in the

74. *See* Botsman, *supra* note 6 (describing in detail the complex standards that the government is setting to rate the behavior of Chinese citizens).

75. *Id.*

76. *Id.*

77. *See id.*

78. *See id.*

79. *See id.* (describing how China's Citizen Score is voluntary now, but will be mandatory by 2020).

80. *See id.*

government nudging citizens away from purchases and behaviors that the government deems negative, such as buying and playing video games.[81] When speech is monitored through social media and online messages, a citizen will be incentivized to say nice things about the Chinese government because it makes their score go up, but if a citizen says something distasteful, not only will that individual's score decrease, but the score of those who are associated with the distasteful speaker will also go down.[82] In addition to the clear incentives to act according to the government's imposed social standards, the system establishes a reward system to further encourage citizens to achieve a higher score.[83] The government, which intends to use high scores as status symbols, will reward those who reach a certain score with "elite" access to loans; VIP check-in at hotels and airports; and the ability to bypass documentation requirements for traveling internationally, such as Singapore.[84]

Botsman emphasizes the effects of such a system by stating that those who choose not to comply with the government's social standards will be penalized.

> [P]eople with low ratings will have slower internet speeds; restricted access to restaurants, nightclubs or golf courses; and the removal of the right to travel freely abroad with, I quote, 'restrictive control on consumption within holiday areas or travel businesses.' Scores will influence a person's rental applications, their ability to get insurance or a loan and even social-security benefits. Citizens with low scores will not be hired by certain employers and will be forbidden from obtaining some jobs, including in the civil service, journalism and legal fields, where of course you must be deemed trustworthy.[85]

Shoshana Zuboff coined the term *surveillance capitalism* when she described the explosion of big data and how the private sector has

---

81. *See id.*

82. *See id.* ("[A] person's own score will also be affected by what their online friends say and do, beyond their own contact with them. If someone they are connected to online posts a negative comment, their own score will also be dragged down.").

83. *See id.*

84. *See id.* ("I think the best way to understand the system is as a sort of bastard love child of a loyalty scheme." (quoting Rogier Creemers)).

85. *Id.* ("In February 2017, [China's] Supreme People's Court announced that 6.15 million of its citizens had been banned from taking flights over the past four years for social misdeeds.").

exploited big data to predict and modify human behavior—all to increase profit.[86] China's leading companies in *surveillance capitalism* are data giants that are dangerously flirting with China's dynamic of communist oversight and capitalist can-do.[87] China Rapid Finance and Sesame Credit, the data giants, are developing systems and algorithms that would grant the Chinese government overarching power to spy on and control the citizenry.[88] A government that monitors the daily activities of their citizens—what they buy, read, watch, post on social media, who they talk to, where they go, how much time they spend playing video games—seems insane, even radical. But what is equally profound is the realization that the United States is not too far away from such a surveillance state.

Evidently, American and Chinese privacy values drastically differ. When Westerners hear about China's social scoring system, they may be appalled by the level of governmental control and the privacy invasions. Yet, the mass data collection capabilities in the United States have parallels to China's system. In addition to FICO scores, which determines many financial decisions such as whether a U.S. citizen can get a loan or buy a house,[89] the United States utilizes a numerical rating scale for restaurants, movies, books, and even doctors.[90] Algorithms are abundant in the United States—from Facebook's facial recognition for automatically tagging people in pictures to the National Security Agency using predictive algorithms to determine who is a threat or risk.[91] Technology and the socialization to accept privacy invasions of technological resources is gradually moving the United States closer to the Chinese system.

In defense of such predictions, one may assert that even if the technology can achieve the same type of mass data collection as China's system, certainly U.S. laws would not allow for such government intrusion and privacy invasions. The United States puts more value on freedom from government intrusion compared to China; but if U.S. case law is applied to China's social credit system in certain contexts, China's tactics may not be deemed unconstitutional.

First, under the Third-party Doctrine, the majority of the data the Chinese government wants to collect is already in the possession of

---

86. *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 75-76 (2015).

87. *See* Botsman, *supra* note 6.

88. *See id.*

89. *See id.* (discussing how credit scores have been around for more than seventy years in the United States but such a system has not existed in China since the majority of Chinese citizens cannot get credit, or credit history).

90. *See id.*

91. *See id.*

third parties, which would lack U.S. Fourth Amendment protections.[92] Data disclosed to a third party includes all activity conducted online (purchases, searches, posts, messages), on a telephone, with a bank, and between a customer and merchant.[93] Despite the autonomy trap of utilizing phone carriers and the Internet, courts still view individuals as voluntarily disclosing information to third parties, thereby waiving any privacy rights.[94]

Second, under a content-or-no-content-based analysis, some of the data the Chinese government desires to access would be unprotected. Courts heavily depend on the content-or-no-content distinction when analyzing cases regarding cell site location information (CSLI).[95] Cell phone tower data discloses where an individual's phone was and provides the individual's location within a narrow but imprecise radius.[96] Because the tower data only reveals the location and not the content of an individual's communications, police can obtain the data without a warrant.[97] The court emphasized the distinction between content and no-content by assessing whether the data obtained by the government was the content of the message itself or no-content information that merely disclosed the data that was necessary to relay the message.[98] In *United States v. Forrester*, the court held that there was no Fourth Amendment search where the government installed a mirror port with only permission for a pen register, rather than a warrant.[99] A mirror port enables government surveillance of the sender

92. *See* United States v. Miller, 425 U.S. 435, 436-37 (1976) (holding that a person who discloses information to a third-party assumes the risk that the information disclosed will be provided to the government).

93. This is not an exhaustive list of information that individuals disclose to third-parties, but a few examples of information that is vital to operating in society.

94. *See* Smith v. Maryland, 442 U.S. 735, 748-50 (1979) (Marshall, T., dissenting) ("It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.").

95. *See generally* United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) (noting that the Supreme Court recognizes a distinction between the content of a communication and the information necessary to convey it); *see also generally* Zanders v. Indiana, 73 N.E.3d 178 (Ind. 2017) (discussing that the distinction between content and no-content determines whether Fourth Amendment protections are extended).

96. *See* Zanders, 73 N.E. 3d at 182 (noting that this case involved only "historical, active, network-based CSLI," not the content of defendant's communications or any high-resolution location data).

97. *See* Carpenter, 819 F.3d at 888 ("[The government] did 'not acquire the *contents* of communications.' . . . [T]he defendants' cellphones signaled the nearest cell towers—thereby giving rise to the data obtained by the government here—solely 'as means of establishing communication.'") (quoting Smith v. Maryland, 442 U.S. 735, 741 (1979)).

98. *See id.* at 887 (describing how no-content, delivery data is like the mailing address on an envelope, which does not disclose the message, or content, inside).

99. *See* United States v. Forrester, 512 F.3d 500, 509-11 (9th Cir. 2008).

and receiver addresses of the defendant's email messages, the IP addresses of the visited websites, and the total volume of information transmitted to or from the account. The court found the mirror port was analogous to a pen register and declared that the to-and-from addresses of an email message and IP addresses of websites do not reveal the content of the message; therefore, the mirror port does not constitute a search under the Fourth Amendment.[100] Collection of no-content data in China, such as location data, emails, and internet searches, would most likely survive the U.S. constitutional test.

Both in the United States and China, mass data collection threatens the dignity and inviolate personality of the citizenry. Consistent with Spiros Simitis's assertions regarding data collection, China is exploiting big data and personal information to enforce standards of behavior through the social credit score regime.[101] The aggregation of data amounts to government surveillance that bestows extreme government and commercial power over citizens. Knowing that the government is constantly tracking daily activities and that each personal decision can affect a social score, individual autonomy and expression will be drastically chilled.[102]

CONCLUSION

Axon profits from further saturating society with cameras, which in turn aids the government in surveillance of its citizenry. Although the criminal investigation tools, such as: Evidence.com or Cop Dropbox; facial recognition; and algorithms that can anticipate criminal activity may reduce costs for detective bureaus and enhance the country's crime-solving capabilities, it should not be deployed without limitations on the government's use. The reasonable expectation of privacy test, the content-or-no-content distinction, and the Third-party Doctrine are inadequate Fourth Amendment points of analysis as technology rapidly enhances. Applying technologies and situations in the information age against the current doctrinal backdrop contributes to the deterioration of information privacy because the application lacks adequate

100. *See id.* at 511.

101. *See* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709-10 (1987) (describing how modern forms of data collection have altered privacy considerations, such as surveillance has lost its prominence because it becomes more and more embedded in our daily routines. Also, information processing is developing into an essential key for strategic manipulation of individual conduct).

102. *See generally id.*, *supra* note 99 (discussing how strengthening the social control threatens the core of democracy); *see also* Richards, *supra* note 45 (discussing the chilling effects that surveillance has on freedom of expression, specifically relating to intellectual expression).

protections for individual privacy. The enhancement of technology, coupled with the stagnate Fourth Amendment points of analysis, has led to the socialization of younger generations to accept less privacy throughout their daily activities since the courts are operating on a circular analysis of societal expectations. Without doctrinal change to limit technologies like Axon's evidence gathering portal, which essentially establishes a perpetual line-up, the technologies will continue to erode the expectation of privacy.

Given that the judicial tests for analyzing cases that concern personal information do not adequately protect individual privacy, a successful implementation of China's social scoring system in the United States is not so farfetched. If a system that had parallels to the social score system underway in China were to be initiated in the United States and subsequently constitutionally challenged, the current Supreme Court jurisprudence would likely be inadequate to fully protect the privacy of citizens' information. The judicially created paradigms such as the reasonable expectation of privacy, Third-party Doctrine, and the content-or-no-content-based distinction all give way to mass data collection and continue to influence the interrelated and often tenuous relationship between privacy and the law.